Discrete abstractions of hybrid systems for verification

George J. Pappas
Departments of ESE and CIS
University of Pennsylvania
pappasg@ee.upenn.edu
http://www.seas.upenn.edu/~pappasg

DISC Summer School on
Modeling and Control of Hybrid Systems
Veldhoven, The Netherlands
June 23-26, 2003

http://lcewww.et.tudelft.nl/~disc_hs/
Outline of this mini-course

Lecture 1: Monday, June 23
   Examples of hybrid systems, modeling formalisms
Lecture 2: Monday, June 23
   Transitions systems, temporal logic, refinement notions
Lecture 3: Tuesday, June 24
   Discrete abstractions of hybrid systems for verification
Lecture 4: Tuesday, June 24
   Discrete abstractions of continuous systems for control
Lecture 5: Thursday, June 26
   Bisimilar control systems
Hybrid to discrete (Lecture 3)

Goal: Finite quotients of hybrid systems
Hybrid System Model

A hybrid system \( H = (V, \mathbb{R}^n, X_0, F, Inv, R) \) consists of

- \( V \) is a finite set of states
- \( \mathbb{R}^n \) is the continuous state space
- \( X = V \times \mathbb{R}^n \) is the state space of the hybrid system
- \( X_0 \subseteq X \) is the set of initial states
- \( F(l, x) \subseteq \mathbb{R}^n \) maps a diff. inclusion to each discrete state
- \( Inv(l) \subseteq \mathbb{R}^n \) maps invariant sets to each discrete state
- \( R \subseteq X \times X \) is a relation capturing discontinuous changes

Define

\[
E = \{(l, l') \mid \exists x \in Inv(l), x' \in Inv(l') \ (l, x), (l', x') \in R\}
\]

\[
Init(l) = \{x \in Inv(l) \mid (l, x) \in X_0\}
\]

\[
Guard(e) = \{x \in Inv(l) \mid \exists x' \in Inv(l') \ (l, x), (l', x') \in R\}
\]

\[
Reset(e, x) = \{x' \in Inv(l') \mid ((l, x), (l', x')) \in R\}
\]
An example

- **Rod1**
  - $\dot{T} = 0.1 \cdot T - 56$
  - $y_1 = 1, y_2 = 1$
  - $T \geq 510$

- **NoRod**
  - $\dot{T} = 0.1 \cdot T - 50$
  - $y_1 = 1, y_2 = 1$
  - $T \leq 550$

- **Rod2**
  - $\dot{T} = 0.1 \cdot T - 60$
  - $y_1 = 1, y_2 = 1$
  - $T \geq 510$

- **Shutdown**
  - $\dot{T} = 0.1 \cdot T - 50$
  - $y_1 = 1, y_2 = 1$
  - true
Transitions of Hybrid Systems

Hybrid systems can be embedded into transition systems

\[ H = (V, \mathbb{R}^n, X_0, F, Inv, R) \quad \longrightarrow \quad T_H = (Q, Q_0, \Sigma, \rightarrow, O, < \cdot >) \]

\[ Q = V \times \mathbb{R}^n \]
\[ Q_0 = X_0 \]
\[ \Sigma = E \cup \{ \tau \} \]
\[ \rightarrow \subseteq Q \times \Sigma \times Q \]

Observation set and map depend on desired properties

<table>
<thead>
<tr>
<th>Discrete transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>((l_1, x_1) \xrightarrow{e} (l_2, x_2)) \iff (x_1 \in \text{Guard}(e), x_2 \in \text{Reset}(e, x_1))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Continuous (time-abstract) transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>((l_1, x_1) \xrightarrow{\tau} (l_2, x_2)) \iff (l_1 = l_2) \ and \ \exists \delta \geq 0 \ \ x(\cdot) : [0, \delta] \rightarrow \mathbb{R}^n \</td>
</tr>
<tr>
<td>(x(0) = x_1, x(\delta) = x_2, \ \text{and} \ \forall t \in [0, \delta] \</td>
</tr>
<tr>
<td>(\dot{x} \in F(l_1, x(t)) \ \text{and} \ x(t) \in Inv(l_1) )</td>
</tr>
</tbody>
</table>
Rectangular hybrid automata

Rectangular sets: $\bigwedge_i x_i \sim c_i \sim \in \{<, \leq, =, \geq, >\}, c_i \in Q$

Rectangular hybrid automata are hybrid systems where

$$Init(l), Inv(l), F(l, x), Guard(e), Reset(e, x)_i$$

are rectangular sets
Multi-rate automata

Multi-rate automata are rectangular hybrid automata where

\[ \text{Init}(l), F(l, x), \text{Reset}(e, x)_i \]

are singleton sets.
Timed automata are multi-rate automata where

\[ F(l, x_i) = 1 \]

for all locations \( l \) and all variables.
Rectangular hybrid automata are initialized if the following holds:

After a discrete transition, if the differential inclusion (equation) for a variable changes, then the variable must be reset to a fixed interval.

Timed automata are always initialized.
Undecidability barriers

Consider the class of uninitialized multi-rate automata with n-1 clock variables, and one two slope variable (with two different rates).

The reachability problem is undecidable for this class.

No algorithmic procedure exists.

Model checking temporal logic formulas is also undecidable

Initializtion is necessary for decidability
Timed automata

All timed automata admit a finite bisimulation

Hence CTL* model checking is decidable for timed automata
Timed automata

Approach: Discretize the clock dynamics using region equivalence
Region equivalence

Equivalence classes: 6 corner points
14 open line segments
8 open regions
Multi-rate automata

All initialized multi-rate automata admit a finite bisimulation
Rectangular automata

All initialized rectangular automata admit a finite bisimulation
All initialized rectangular automata admit a finite bisimulation.
No finite bisimulation

Bisimulation algorithm never terminates
All initialized rectangular automata admit a finite language equivalence quotient which can be constructed effectively.

LTL model checking of rectangular automata is decidable.
More complicated dynamics?

Sets
\[ P_1 = \{(x,0) \mid 0 \leq x \leq 4\} \]
\[ P_2 = \{(x,0) \mid -4 \leq x < 0\} \]
\[ P_3 = \mathbb{R}^2 \setminus (P_1 \cup P_2) \]

Dynamics
\[ \dot{x}_1 = 0.2x_1 + x_2 \]
\[ \dot{x}_2 = -x_1 + 0.2x_2 \]
Basic problems

Finite bisimulations of continuous dynamical systems

Given a vector field $F(x)$ and a finite partition of $\mathbb{R}^n$

1. Does there exist a finite bisimulation?
2. Can we compute it?
Reminder

Representation issues
- Symbolic representation for infinite sets
- Rectangular sets? Semi-linear? Semi-algebraic?

Operations on sets
- Boolean (logical) operations
  - Can we compute Pre and Post?
  - Is our representation closed under Pre and Post?

Algorithmic termination (decidability)
- No guarantee for infinite transition systems
- We need “nice” alignment of sets and flows
- Globally finite properties
First-order logic

Every theory of the reals has an associated language

\[(\mathbb{R}, <, +, -, 0, 1)\]

Universe Relation Functions Constants

Variables: \(x_1, x_2, x_3, \ldots\)

**TERMS:** Variables, constants, or functions of them
\[x_1 - x_2 + 1, 1 + 1, -x_3\]

**ATOMIC FORMULAS:** Apply the relation and equality to the terms
\[x_1 + x_2 < -1, 2x_1 = 1, x_1 = x_3\]

**(FIRST ORDER) FORMULAS:** Atomic formulas are formulas
If \(\varphi_1, \varphi_2\) are formulas, then \(\varphi_1 \lor \varphi_2, \neg \varphi_1, \forall x. \varphi_1, \exists x. \varphi_1\)
First-order logic

Useful languages

\( (\mathbb{R}, <, +, -, 0, 1) \)
\[ \forall x \forall y (x + 2y \geq 0) \]

\( (\mathbb{R}, <, +, -, \times, 0, 1) \)
\[ \exists x. ax^2 + bx + c = 0 \]

\( (\mathbb{R}, <, +, -, \times, e^x, 0, 1) \)
\[ \exists t. (t \geq 0) \land (y = e^{tx}) \]

A theory of the reals is **decidable** if there is an algorithm which in a finite number of steps will decide whether a formula is true or not.

A theory of the reals admits **quantifier elimination** if there is an algorithm which will eliminate all quantified variables.

\[ \exists x. ax^2 + bx + c = 0 \equiv b^2 - 4ac \geq 0 \]
First-order logic

<table>
<thead>
<tr>
<th>Theory</th>
<th>Decidable ?</th>
<th>Quant. Elim. ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\mathbb{R}, &lt;, +, -, 0, 1)$</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>$(\mathbb{R}, &lt;, +, -, \times, 0, 1)$</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>$(\mathbb{R}, &lt;, +, -, \times, e^x, 0, 1)$</td>
<td>?</td>
<td>NO</td>
</tr>
</tbody>
</table>

**Tarski's result**: Every formula in $(\mathbb{R}, <, +, -, \times, 0, 1)$ can be decided
1. Eliminate quantified variables
2. Quantifier free formulas can be decided
**O-Minimal Theories**

A definable set is

\[ Y = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid \varphi(x_1, \ldots, x_n)\} \]

A theory of the reals is called **o-minimal** if every definable subset of the reals is a **finite** union of points and intervals.

Example: \[ Y = \{(x) \in \mathbb{R} \mid p(x) \geq 0\} \] for polynomial \( p(x) \)

Recent o-minimal theories

- \((\mathbb{R}, <, +, -, 0, 1)\)
- \((\mathbb{R}, <, +, -, \times, 0, 1)\)
- \((\mathbb{R}, <, +, -, \times, e^x, 0, 1)\) Related to Hilbert’s 16th problem
- \((\mathbb{R}, <, +, -, \times, \hat{f}, 0, 1)\)
- \((\mathbb{R}, <, +, -, \times, \hat{f}, e^x, 0, 1)\)
Finite bisimulations of continuous dynamical systems

Consider a vector field $X$ and a finite partition of $\mathbb{R}^n$ where

1. The flow of the vector field is definable in an o-minimal theory
2. The finite partition is definable in the same o-minimal theory

Then a finite bisimulation always exists.
Corollaries

Consider continuous systems where
- Finite partition is polyhedral (semi-linear)
- Vector fields have linear flows (timed, multi-rate)

Then a finite bisimulation exists.

Consider continuous systems where
- Finite partition is semialgebraic
- Vector fields have polynomial flows

Then a finite bisimulation exists.
Corollaries

Consider continuous systems where

- Finite partition is semi-algebraic
- Vector fields are linear with real eigenvalues

Then a finite bisimulation exists.

Consider continuous systems where

- Finite partition is sub-analytic
- Vector fields are linear with purely imaginary eigenvalues

Then a finite bisimulation exists.
Consider continuous systems where

- Finite partition is semi-algebraic
- Vector fields are linear with real or imaginary eigenvalues

Then a finite bisimulation exists.

Conditions are sufficient but tight.
Computability

Finite bisimulations exist, but can we compute them?

Bisimulation Algorithm

initialize $Q/\sim = \{ p \sim q \text{ } \text{iff} \text{ } <q> = <p> \}$

while $\exists P, P' \in Q/\sim$ such that $\emptyset \not\subseteq P \cap \text{Pre}(P') \not\subseteq P$

$P_1 := P \cap \text{Pre}(P')$

$P_2 := P \setminus \text{Pre}(P')$

$Q/\sim := (Q/\sim \setminus \{ P \}) \cup \{ P_1, P_2 \}$

end while

Need to: Check emptiness
Perform boolean operations
Compute Pre (or Post)

Use $(\mathcal{R}, \langle, +, -, \times, 0, 1)$
Computing reachable sets

Consider a linear system

\[
\frac{dx}{dt} = Ax \quad A \in \mathbb{Q}^{n \times n}
\]

and a semi-algebraic set \( Y \). If

\[
Y = \{ y \in \mathbb{R}^n \mid p(y) \}
\]

Then

\[
\text{Pre}(Y) = \{ x \in \mathbb{R}^n \mid \exists y \exists t. p(y) \land t \geq 0 \land x = e^{-tA}y \}
\]
Nilpotent Linear Systems

Nilpotent matrices: \( \exists n \geq 0 \ A^n = 0 \)

Then flow of linear system is polynomial

\[
e^{-tA} = \sum_{k=0}^{n-1} (-1)^{k} \frac{k^t}{k!} A^k
\]

Therefore \( \text{Pre}(Y) \) completely definable in \( (\mathbb{R},<,+,-,\times,0,1) \)

\[
\text{Pre}(Y) = \{ x \in \mathbb{R}^n \mid \exists y \exists t. p(y) \land t \geq 0 \land x = \sum_{k=0}^{n-1} (-1)^k \frac{k^t}{k!} A^k y \}
\]
Diagonalizable, rational eigenvalues

Example system: \[ \dot{x} = 2x \]

Compute all states that can reach the set \( Y = \{ y=5 \} \)

\[ Pre(Y) = \{ x \in \mathbb{R} \mid \exists y \exists t. y = 5 \land t \geq 0 \land x = e^{-2t}y \} \]

Let \( s = e^{-t} \), then

\[ Pre(Y) = \{ x \in \mathbb{R} \mid \exists y \exists t. y = 5 \land 1 \geq s \geq 0 \land x = s^2y \} \]

\[ Pre(Y) = \{ x \in \mathbb{R} \mid 0 < x \leq 5 \} \]
Diagonalizable, rational eigenvalues

More generally \( \dot{x} = Ax \Rightarrow x(t) = Te^{At}T^{-1}x(0) \)

Therefore \( e^{-tA} = \left[ \sum_{k=1}^{n} a_{ijk}e^{-\lambda_k t} \right]_{ij} \)

1. Rescale rational eigenvalues to integer eigenvalues.
2. Eliminate negative integer eigenvalues.
3. Perform the substitution \( s = e^{-t} \)

Consider diagonalizable linear vector fields with real, rational eigenvalues, and let \( Y \) be a semi-algebraic set. Then \( \text{Pre}(Y) \) is also semi-algebraic (and computable)
Diagonalizable, imaginary eigenvalues

Procedure is similar if system is diagonalizable with purely imaginary, rational eigenvalues

Equivalence is obtained by \( z_1 = \cos(t) \quad z_2 = \sin(t) \)

Suffices to compute over a period

Consider diagonalizable linear vector fields with real, rational eigenvalues, and let \( Y \) be a semi-algebraic set. Then \( \text{Pre}(Y) \) is also semi-algebraic (and computable)

Composing all computability results together results in...
Decidable problems for continuous systems

Consider linear vector fields of the form $F(x) = Ax$ where

- $A$ is rational and nilpotent
- $A$ is rational, diagonalizable, with rational eigenvalues
- $A$ is rational, diagonalizable, with purely imaginary, rational eigenvalues

Then

1. The reachability problem between semi-algebraic sets is decidable.

2. Consider a finite semi-algebraic partition of the state space. Then a finite bisimulation always exists and can be computed.

3. Consider a CTL* formula where atomic propositions denote semi-algebraic sets. Then CTL* model checking is decidable.
A hybrid system $H$ is said to be o-minimal if

1. In each discrete state, all relevant sets and the flow of the vector field are definable in the same o-minimal theory.
2. After every discrete transition, state is reset to a constant set (forced initialization)

All o-minimal hybrid systems admit a finite bisimulation.

CTL* model checking is decidable for the class of o-minimal hybrid systems.
Decidable problems for hybrid systems

Consider a linear hybrid system $H$ where

1. For each discrete state, all relevant sets are semi-algebraic
2. After every discrete transition, state is reset to a constant semi-algebraic set (forced initialization)
3. In each discrete location, the vector fields are of the form $F(x) = Ax$ where
   - $A$ is rational and nilpotent
   - $A$ is rational, diagonalizable, with rational eigenvalues
   - $A$ is rational, diagonalizable, with purely imaginary, rational eigenvalues

Then

$\text{CTL}^*$ model checking is decidable for this class of linear hybrid systems.

The reachability problem is decidable for such linear hybrid systems.
Safety games

Consider the following differential game

$$\dot{x} = Ax + Bu + Ed \quad u \in U \quad d \in D$$

Objective for control : Remain in semi-algebraic set $F$
Objective for disturbance : Exit semi-algebraic set $F$

$$F = \{ x \in \mathbb{R}^n \mid h(x) > 0 \}$$

Winning set for $u$

$$\forall d(t) \exists u(t) \quad \square x(t) \in F$$

Winning set for $d$

$$\exists d(t) \forall u(t) \quad \Diamond x(t) \not\in F$$
Optimal control

The Hamiltonian

$$H(x, p, u, d) = p^T A x + p^T B u + p^T E d$$

must satisfy the Hamilton-Jacobi-Isaacs condition

$$\max_{u \in U} \min_{d \in D} H(x, p, u, d) = \min_{d \in D} \max_{u \in U} H(x, p, u, d)$$

Optimum (bang-bang) policies satisfy

$$\dot{x} = \frac{\partial H}{\partial p}$$

$$\dot{p} = \left( \frac{\partial H}{\partial x} \right)^T$$

$$u^* = \arg \max_{u \in U} p^T B u$$

$$d^* = \arg \min_{d \in D} p^T E d$$

$$p(x, 0) = \frac{\partial h}{\partial x}$$
Encoding game as hybrid system

$q_0 = (0, 0)$

\[ \dot{x} = Ax + Bu + Ed \]

\[ \dot{p} = A^T p \]

\[ (p^T B < 0) \land (p^T E < 0) \]

$q_1 = (0, 1)$

\[ \dot{x} = Ax + Bu + \bar{E}d \]

\[ \dot{p} = A^T p \]

\[ (p^T B < 0) \land (p^T E > 0) \]

$q_2 = (1, 0)$

\[ \dot{x} = Ax + B\bar{u} + Ed \]

\[ \dot{p} = A^T p \]

\[ (p^T B > 0) \land (p^T E < 0) \]

$q_3 = (1, 1)$

\[ \dot{x} = Ax + B\bar{u} + \bar{E}d \]

\[ \dot{p} = A^T p \]

\[ (p^T B > 0) \land (p^T E > 0) \]
Pontryagin Maximum Principle

A linear system \( \dot{x} = Ax + Bu \) is normal if for each input column \( b_i \), the pair \( (A, b_i) \) is completely controllable.

If the linear system is normal with respect to both control and disturbance, then for any initial state the optimal control and optimal disturbance are well-defined, unique and piece-wise constant taking values on the vertices of \( U \) and \( D \).

If the linear system is normal and \( A \) has purely real eigenvalues, then there is a global, uniform upper bound, independent of the initial state on the number of switchings of the optimal control and optimal disturbance.
Decidable games

Combining optimal control and decidable logics we get...

Consider the differential game
\[
\dot{x} = Ax + Bu + Ed \quad u \in U \quad d \in D
\]
with target set
\[
F = \{ x \in \mathbb{R}^n \mid h(x) > 0 \}
\]
If the system is normal and A has real eigenvalues, then the differential game can be decided.

Winning sets for u and d can be computed.
Least restrictive controllers can be computed.
Extension to chained form

Consider chained system

\[
\begin{align*}
\dot{x}^0_j &= u_j & j &= 1, \ldots, m \\
\dot{x}^1_{ij} &= x^0_i u_j & j &= 1, \ldots, m \text{ and } i < j \\
\dot{x}^k_{ij} &= x^{k-1}_{ij} u_j & j &= 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j.
\end{align*}
\]

Construct Hamiltonian

\[
H(x, p, u) = p^T f(x, u) = \sum_{j=1}^{m} \left( p_j^0 + \sum_{i=1}^{j-1} (p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1}) \right) u_j
\]

Co-state dynamics

\[
\begin{align*}
\dot{p}_{ij}^n & = 0 & j &= 1, \ldots, m \text{ and } i < j \\
\dot{p}_{ij}^{k-1} & = -p_{ij}^k u_j & j &= 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}_i^0 & = -\sum_{j=1}^{m} p_{ij}^1 u_j & i &= 1, \ldots, m.
\end{align*}
\]

Optimal control satisfies maximum principle:

\[
u_j^* = \arg \max_{u_j \in [\underline{U}_j, \overline{U}_j]} \left( p_j^0 + \sum_{i=1}^{j-1} (p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1}) \right) u_j
\]
Polynomial flows

Dynamics in discrete state (optimal input is constant)

\[ \begin{align*}
\dot{x}^0_{ij} &= u^*_j & j &= 1, \ldots, m \\
\dot{x}^1_{ij} &= x^0_{ij} u^*_j & j &= 1, \ldots, m \text{ and } i < j \\
\dot{x}^k_{ij} &= x^{k-1}_{ij} u^*_j & j &= 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}^n_{ij} &= 0 & j &= 1, \ldots, m \text{ and } i < j. \\
\dot{p}^{k-1}_{ij} &= -p^k_{ij} u^*_j & j &= 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}^0_i &= -\sum_{j=1}^{m} p^1_{ij} u^*_j & i &= 1, \ldots, m.
\end{align*} \]

Polynomial flow in each discrete state

\[ \begin{align*}
x^0_i(t) &= x^0_i(0) + u^*_i t & i &= 1, \ldots, m \\
x^1_{ij}(t) &= x^1_{ij}(0) + x^0_i(0) u^*_j t + \frac{1}{2} u^*_i u^*_j t^2 \\
&\vdots \\
p^n_{ij}(t) &= p^n_{ij}(0) & j &= 1, \ldots, m \text{ and } i < j \\
p^k_{ij}(t) &= \sum_{l=0}^{n_j-k} \frac{(-u^*_j t)^l}{l!} p^{k+l}_{ij}(0) & j &= 1, \ldots, m \text{ and } i < j \text{ and } k = 1, \ldots, n_j \\
p^0_i(t) &= p^0_i(0) + \sum_{l=1}^{n_j-1} \frac{(-u^*_i t)^l}{l!} p^l_{ij}(0) & i &= 1, \ldots, m.
\end{align*} \]
Conflict Resolution in ATM*
Conflict Resolution Protocol

1. Cruise until $a_1$ miles away
2. Change heading by $\Delta \Phi$
3. Maintain heading until lateral distance $d$
4. Change to original heading
5. Change heading by $-\Delta \Phi$
6. Maintain heading until lateral distance $-d$
7. Change to original heading

Is this protocol safe?
Conflict Resolution Maneuver

**CRUISE**
Dynamics
\[
\begin{align*}
\dot{x} &= -v_1 + v_2 \cos(\phi_2 - \phi_1) \\
\dot{y} &= v_2 \sin(\phi_2 - \phi_1) \\
\dot{t} &= 0
\end{align*}
\]
Invariant
\[x^2 + y^2 \geq \alpha_1\]

**LEFT**
Dynamics
\[
\begin{align*}
\dot{x} &= -v_1 + v_2 \cos(\phi_2 - \phi_1) \\
\dot{y} &= v_2 \sin(\phi_2 - \phi_1) \\
\dot{t} &= 1
\end{align*}
\]
Invariant
\[t \leq \frac{2d}{v_1 + v_2 \sin(\Delta \phi)}\]

**RIGHT**
Dynamics
\[
\begin{align*}
\dot{x} &= -v_1 + v_2 \cos(\phi_2 - \phi_1) \\
\dot{y} &= v_2 \sin(\phi_2 - \phi_1) \\
\dot{t} &= 0
\end{align*}
\]
Invariant
\[t \geq 0\]

**STRAIGHT**
Dynamics
\[
\begin{align*}
\dot{x} &= -v_1 + v_2 \cos(\phi_2 - \phi_1) \\
\dot{y} &= v_2 \sin(\phi_2 - \phi_1) \\
\dot{t} &= t
\end{align*}
\]
Invariant
\[x^2 + y^2 \leq \alpha_2\]
### Computing Unsafe Sets

<table>
<thead>
<tr>
<th>unsafeCruise</th>
<th>$v_1 = 4; v_2 = 5; \lambda = 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists t &gt; 0 \land (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1 - \lambda^2} v_2 t)^2 \leq 25$</td>
<td></td>
</tr>
<tr>
<td>$\lor (y = -\frac{20}{\sqrt{41}} \land -\frac{4y}{5} &lt; x \leq \sqrt{41} - \frac{4y}{5}) \lor (y = \frac{20}{\sqrt{41}} \land -\frac{25}{4} - y^2 &lt; x &lt; \sqrt{25} - y^2) \lor (-\frac{20}{\sqrt{41}} &lt; y &lt; \frac{20}{\sqrt{41}} \land -\frac{25}{4} - y^2 &lt; x \leq \sqrt{41} - \frac{4y}{5})$</td>
<td></td>
</tr>
</tbody>
</table>

| unsafeLeft | $v_1 = 4; v_2 = 5; \lambda = \frac{3}{5}$ |
| $\exists t > 0 \land (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1 - \lambda^2} v_2 t)^2 \leq 25$ |
| $\lor (y = -\frac{5\sqrt{17}}{4} \land -\frac{5\sqrt{17}}{4} - y \leq x \leq \frac{5\sqrt{17}}{4} - \frac{y}{4}) \lor (y = -\frac{5\sqrt{17}}{4} \land -\frac{5\sqrt{17}}{4} - \frac{y}{4} < x \leq \frac{5\sqrt{17}}{4} - \frac{y}{4}) \lor (-\frac{5\sqrt{17}}{4} < y < \frac{5\sqrt{17}}{4} \land -\sqrt{25} - y^2 < x \leq \frac{5\sqrt{17}}{4} - \frac{y}{4})$ |

| unsafeRight | $v_1 = 4; v_2 = 5; \lambda = -\frac{3}{5}$ |
| $\exists t > 0 \land (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1 - \lambda^2} v_2 t)^2 \leq 25$ |
| $\lor (y = -7\sqrt{\frac{5}{13}} \land -\frac{5\sqrt{65}}{4} - \frac{7y}{4} \leq x \leq \frac{5\sqrt{65}}{4} - \frac{7y}{4}) \lor (y = 7\sqrt{\frac{5}{13}} \land -\sqrt{25} - y^2 < x < \frac{5\sqrt{65}}{4} - \frac{7y}{4}) \lor (-7\sqrt{\frac{5}{13}} < y < 7\sqrt{\frac{5}{13}} \land -\sqrt{25} - y^2 < x \leq \frac{5\sqrt{65}}{4} - \frac{7y}{4})$ |
Safe Sets

(a) unsafeCruise

(b) unsafeLeft

(c) unsafeRight

(d) unsafeCruise ∧ unsafeLeft ∧ unsafeRight
Continuous to discrete (Lectures 3 & 4)

**Lecture 3**

- Restricted dynamical systems
- Semi-algebraic partitions
- Verification semantics

\[
\frac{dx}{dt} = Ax
\]

**Lecture 4**

- Linear control systems
- Restricted partitions
- Synthesis semantics

\[
\frac{dx}{dt} = Ax + Bu
\]